

WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

| | | |
|---------------------------|---|-----------------------|
| United States of America, |) | No. CR 08-814-PHX-DGC |
| |) | |
| Plaintiff, |) | |
| |) | |
| vs. |) | ORDER |
| |) | |
| Daniel David Rigmaiden, |) | |
| |) | |
| Defendant. |) | |

Defendant Daniel Rigmaiden has filed an Amended Motion for Reconsideration. Doc. 1033. Defendant asks the Court to reconsider its order denying his motion to suppress and related motions. Doc. 1009. The Court will deny Defendant's motion.

Motions for reconsideration "are disfavored and will be granted only upon a showing of manifest error or new facts or legal authority which could not have been raised earlier with reasonable diligence." *Arizona Dream Act Coalition v. Brewer*, --- F. Supp.2d ---, 2013 WL 2128315, at *25 (D.Ariz. 2013) (quotations omitted); LRCiv 7.2(g)(1). Mere disagreement with an order is an insufficient basis for reconsideration. *Id.*

Defendant asserts that the Court's order, which addressed his 335-page motion to suppress and thousands of pages of exhibits, contained numerous errors of fact and law. These alleged errors do not entitle Defendant to relief.

I. Alleged Manifest Factual Errors.

Defendant identifies several errors committed by the Court in its discussion of the legitimacy of Defendant's expectation of privacy in his aircard, computer, and apartment.

1 Defendant's arguments concerning these errors do not support his motion for
2 reconsideration.¹

3 Defendant contends that the Court erred in describing several of the false identities
4 he used. Doc. 1033 at 2–3. Specifically, he argues that when he used false driver's license
5 numbers, he was unaware that the numbers were assigned to real, living individuals. *Id.*
6 This argument fails to identify any error and does not affect the Court's finding that
7 Defendant's use of false identities negated any legitimate expectation of privacy in the
8 aircard, computer, and apartment.

9 Defendant claims that he purchased the aircard without providing any name, contrary
10 to the Court's statement that he purchased the card in the name of Travis Rupard. *Id.* at 7.
11 The government acknowledges that it "obtained no information during the investigation
12 about the actual purchase of the aircard." Doc. 1071 at 3. The fact remains, however, that
13 Defendant activated and maintained the aircard under the false identity of Travis Rupard.
14 The fraudulent use of the aircard thus remains a relevant consideration, and the Court's
15 analysis does not change.

16 Defendant argues that the Court erred in stating that Defendant used a fraudulent Visa
17 card to purchase his computer. Doc. 1033 at 8. In fact, Defendant purchased the computer
18 using a fraudulently-obtained prepaid debit card. *See* Doc. 824-3, ¶ 4. This distinction does
19 not alter the Court's analysis.

20 Defendant contends that Court erred in finding that he was prepared to abandon his
21 apartment if he became aware of the government's investigation, and in finding that the
22 contents of his storage unit, including \$70,000 in cash, a false passport, and a hard drive with
23 a backup copy of the contents of his laptop,² provided evidence of Defendant's intent to flee.

25 ¹ The factual and procedural background of the case is described in previous
26 orders, *see* Docs. 723, 1009, and will be repeated here only as necessary.

27 ² In its order denying Defendant's motion to suppress, the Court described the
28 hard-drive as a "computer with back-up information" and a "copy of his laptop computer."

1 *Id.* at 1003–07. According to Defendant, the record shows only that he was prepared to pack
2 up and leave the apartment in a day’s time if he had been served with a warrant. *Id.* at 4–5.
3 That clarification does nothing to change the Court’s conclusion that he was prepared to flee.
4 Indeed, the Court’s finding was based in part on Defendant’s own declaration:

5 Prior to my arrest and search of my home, but after the FBI had located my
6 aircard and residence on July 16-17, 2008, had I been served with copies of
7 relevant orders and receipts of items seized, there would have been nothing for
8 the government to seize and nobody for the government to arrest during the in-
9 person search of apartment No. 1122 on August 3, 2008. Had I received notice
of the aircard locating mission, within a day I would have permanently left
apartment No. 1122 after packing up my belongings and cleaning the
apartment. I would have also permanently stopped using my aircard and
aircard account.

10 Doc. 824-2, ¶ 14.

11 This information, in conjunction with the contents of the storage unit, fully supports
12 the Court’s conclusion that Defendant exhibited a willingness and ability to abandon his
13 apartment and flee the authorities, which in turn supports the Court’s conclusion that
14 Defendant’s expectation of privacy was not one society is prepared to recognize as
15 reasonable.

16 Defendant alleges that the Court made several errors in describing the aircard search.
17 He objects to the characterization of the use of mobile tracking devices as not a “severe
18 intrusion” (Doc. 1033 at 9), arguing that a Fourth Amendment search is by definition a severe
19 intrusion. Defendant misconstrues the Court’s use of the phrase. As noted in the Court’s
20 order denying Defendants’s suppression motion, the Ninth Circuit has held that “the
21 legitimacy of a citizen’s expectation of privacy in a particular place may be affected by the
22 nature of the intrusion that occurs.” *United States v. Nerber*, 222 F.3d 597, 601 (9th Cir.
23 2000). The court of appeals characterized as “severe” the government’s use of hidden video
24 equipment to make video recordings of the defendants in their hotel room. *Id.* at 602. In
25 contrast, the government’s use of a mobile tracking device in this case to send signals to and
26 receive signals from the aircard was not as severe an intrusion, particularly given

27 _____
28 Doc. 1009 at 8, 10.

1 Defendant's use of the same aircard to perpetrate Defendant's fraudulent scheme through
2 electronic communications.

3 Moreover, the Court's observation that the intrusion in this case was not severe when
4 compared to intrusions like those in *Nerber* did not constitute the sole basis, or even an
5 independent basis, for the Court's conclusion that the Fourth Amendment was not violated.
6 Rather, it bore on Defendant's legitimate expectation of privacy (*see id.* at 601) and was cited
7 by the Court as a factor that "strengthened" the conclusion already reached – that Defendant
8 had no legitimate expectation of privacy in the devices and apartment he acquired through
9 fraud. *See* Doc. 1009 at 13. The Court would have reached that conclusion even without this
10 strengthening consideration.

11 Defendant asserts that the Court erred in describing the mobile tracking device as
12 "relatively new technology." Doc. 1033 at 10. Defendant's argument that the technology
13 had been used since the 1990s does not affect the Court's conclusion that, in the context of
14 a Fourth Amendment analysis, the agents involved in the aircard search were faced with a
15 lack of legal precedent in obtaining the proper form of warrant.

16 Defendant disputes the Court's finding that the government was motivated by the
17 protection of third parties when, in compliance with the warrant, it deleted all of the data
18 gathered by the mobile tracking devices. *Id.* at 9. Defendant alleges that the government
19 deleted the data to "hide the details of the device from the defense." *Id.* at 10. This
20 speculation is not supported by the record, *see* Doc. 674-1, ¶ 5 (declaration by FBI special
21 agent stating that policy requires that data be purged to protect the privacy rights of third
22 parties), and has no bearing on the Court's analysis of the government's duty of candor.

23 Defendant states that the Court erred in its description of the process by which the
24 government obtained gate access data for his apartment complex. Doc. 1033 at 11. He does
25 not explain, however, why the details supplied in his motion affect the Court's analysis.

26 Finally, Defendant asserts that the Court erred in describing details of his arrest and
27 the subsequent search of his apartment. Doc. 1033 at 12. Defendant argues, for example,
28

1 that he was actually arrested by Santa Clara police officers (who were assisting federal agents
2 in apprehending Defendant) and that the agent who inserted the key into his lock did not
3 actually participate in the search of his apartment. These factual differences have no effect
4 on the Court's analysis.

5 Having reviewed all of the alleged manifest errors of fact identified by Defendant, the
6 Court finds that none entitles Defendant to relief.

7 **II. Alleged Manifest Legal Errors.**

8 Defendant asserts that the Court made numerous legal errors in its analysis of the
9 tracking warrant and its execution, the reasonableness of his expectation of privacy, and the
10 validity of the computer search. The Court disagrees.

11 **A. Tracking Warrant.**

12 (1) Defendant asserts that the Court ignored his argument that the N.D.Cal. 08-
13 90330-MISC-RS order (the "tracking warrant") was never actually executed. Doc. 1033 at
14 13–15. Alternatively, Defendant contends that there is no evidence that the agents who
15 "purportedly" executed the warrant were familiar with its terms. *Id.* at 13. In support of
16 these arguments, Defendant notes that no return of the warrant was filed, no one was served
17 with the warrant, and the government is unwilling to produce the technical agents who
18 executed the warrant. *Id.* at 13. Defendant further asserts that the government lacked
19 credibility when it represented, at oral argument on the motion to suppress, that it could
20 produce witnesses who spoke with the technical agents and could offer hearsay testimony
21 that the agents were provided a copy of the order and reviewed the order.

22 Defendant's argument that the tracking warrant was not executed is dubious, given
23 his acknowledgment that "Fourth Amendment activity certainly took place," Doc. 900 at
24 48–49, and the fact that the bulk of his arguments concerns the manner in which the warrant
25 *was* executed. Moreover, having found that the search for the aircard did not exceed the
26 scope of the tracking warrant, the Court finds no basis on which to conclude that the agents
27 who executed the warrant were unfamiliar with its terms.

1 (2) Defendant argues that the Court overlooked his argument that the aircard
2 tracking operation consisted of numerous individual searches and seizures, each of which had
3 to be analyzed separately as a Fourth Amendment search or seizure.³ Doc. 1033 at 15-18.
4 In support of this argument, Defendant notes that the government conceded that each of the
5 individual actions identified by Defendant was a search or seizure for Fourth Amendment
6 purposes. *Id.* According to Defendant, these concessions required the Court to make a scope
7 and probable cause determination with respect to each of the separate components of the
8 aircard tracking mission. *Id.*

9 The government's concession that the aircard tracking mission, as well as its
10 individual components, constituted a Fourth Amendment search does not compel the
11 analytical framework urged by Defendant. As the Court explained in its previous order, the
12 Fourth Amendment requires that a warrant be supported by probable cause and that it
13 particularly describe the items to be seized and the places to be searched. *Dalia v. United*
14 *States*, 441 U.S. 238, 255 (1979). There is no requirement that "search warrants also must
15 include a specification of the precise manner in which they are to be executed. On the
16 contrary, it is generally left to the discretion of the executing officers." *Id.* at 257.

17 Defendant cites no authority for his argument that each component of a search
18 undertaken pursuant to a valid warrant must be analyzed separately for scope and probable
19 cause. Nor does he explain how a discrete analysis of the steps involved in the aircard
20 tracking mission would affect the Court's legal conclusions concerning the validity of the
21

22
23 ³ In his motion to suppress, Defendant enumerated 18 different searches or
24 seizures involved in the aircard tracking mission. Doc. 824 at 257–85. These included using
25 the tracking devices "to remotely access and download data from the aircard," "send location
26 finding interrogation signals into the defendant's home and aircard," and "deny the defendant
27 access to the Internet for ten hours." They also included the "FBI using the defendant's
28 electricity provided to his aircard and forcing the aircard to transmit at the highest possible
power." In a status conference on January 27, 2012, the government conceded that these
various activities constituted searches under the Fourth Amendment, assuming Defendant had
a legitimate expectations of privacy in the places and items searched. Doc. 776 at 19, 22.

1 tracking warrant or the manner in which it was executed. Having found that the warrant
2 satisfied the probable cause and particularity requirements, and that the agents did not exceed
3 the scope of the warrant, the Court also finds that the individual actions comprising the
4 aircard tracking mission were supported by probable cause and within the scope of the
5 warrant.

6 (3) Defendant argues that agents exceeded the scope of the tracking warrant by
7 using two different mobile tracking devices, including a “*second*, handheld ‘mobile tracking
8 device’ within the Domicilio apartment complex.” Doc. 1033 at 24 (emphasis in original).
9 According to Defendant, the Court erred by failing to suppress evidence obtained through
10 use of the second device. *Id.* The Court disagrees. The use of a second mobile tracking
11 device did not broaden the scope of the authorized search. Defendant cites *United States v.*
12 *Chen*, 979 F.2d 714 (9th Cir. 1992), but *Chen* found that suppression was not the appropriate
13 remedy where the government exceeded the scope of the warrant by using a second and third
14 camera for video surveillance. The court concluded that the use of additional cameras was
15 “motivated by considerations of practicality rather than by a desire to engage in
16 indiscriminate ‘fishing.’” *Id.* at 718. Here, the agents used both tracking devices to locate
17 the aircard, which was the object to the search. They did not exceed the scope of the warrant.

18 (4) Defendant argues that the “operative section” of the warrant did not authorize
19 anyone to use a mobile tracking device. Doc. 1033 at 24. Defendant simply disagrees with
20 the Court’s characterization of the warrant, which specifically authorizes the use of a mobile
21 tracking device. Moreover, Defendant’s interpretation does not survive a common sense
22 reading of the document. *See United States v. Marques*, 600 F.2d 742, 751 (9th Cir. 1979)
23 (noting “it is by now almost a cliché that affidavits submitted in support of applications for
24 search warrants are to be read in a common-sense, non-technical manner”). Defendant’s
25 reliance on *United States v. Robinson*, 358 F. Supp.2d 975 (D. Mont. 2005), is misplaced.
26 There, the operative portion of the warrant authorized the search of the defendant’s pickup
27 truck, but did not explicitly authorize a search of her residence. The search of the residence
28

1 therefore exceeded the scope of the warrant. Here, the tracking warrant described the
2 aircard with particularity and agents did not exceed the scope of the authorized search.

3 (5) Defendant argues that the Court erred in its application of *Dalia* to the
4 “separate issue of the government failing to describe its surveillance technology in the
5 [tracking warrant].” Doc. 1033 at 25 (emphasis in original). Defendant cites *United States*
6 *v. Oliva*, 705 F.3d 390, 394 (9th Cir. 2012), as “controlling Ninth Circuit case law effectively
7 distinguishing *Dalia* from searches and seizures involving new surveillance technology.”
8 Doc. 1033 at 26–27. In its order denying Defendant’s motion to suppress, the Court fully
9 addressed the arguments, raised by Defendant and the ACLU, that the warrant lacked
10 particularity and the government violated its duty of candor by failing to disclose additional
11 technical details of the mobile tracking device. Doc. 1009 at 25–33. Defendant has
12 identified no error and the Court need not rethink its analysis at Defendant’s behest. *Arizona*
13 *Dream Act Coalition*, --- F. Supp.2d ---, 2013 WL 2128315, at *25.

14 Moreover, *Oliva* does not impose an additional requirement on warrants seeking to
15 use new technology. Instead, the court in *Oliva* addressed a specific technological issue, the
16 conversion of cell phones into “roving bugs,” and held that “[b]efore the government can
17 employ technologies that can eavesdrop on background conversations even if the cell phone
18 is ‘off’ . . . it would have to comply with the statutory requirements for such intrusive
19 surveillance.” 705 F.3d at 399. The holding in *Oliva* does not disturb this Court’s
20 conclusion, pursuant to *Dalia*, that the government was not obligated to provide additional
21 technical details about the operation of the mobile tracking device.

22 (6) Defendant argues that the Court erred by considering the affidavit of Agent Ng
23 when analyzing Defendant’s scope and particularity challenges to the tracking warrant.
24 According to Defendant, the affidavit was not incorporated by reference into the warrant and
25 did not accompany the agents during the tracking operation. Doc. 1033 at 27–28.

26 A search warrant “may be construed with reference to the affidavit for purposes of
27 satisfying the particularity requirement if (1) the affidavit accompanies the warrant, and (2)
28

1 the warrant uses suitable words of reference which incorporate the affidavit therein.” *United*
2 *States v. Hillyard*, 677 F.2d 1336, 1340 (9th Cir. 1982). The tracking warrant states that the
3 “matter is before the Court pursuant to an Application . . . by Assistant United States
4 Attorney Shawna Yen[.]” Doc. 470-1. Attached to the Application is Agent Ng’s affidavit.
5 *Id.* Other than the available hearsay testimony described by the government during oral
6 argument, there is no evidence as to whether the technical agents possessed the affidavit
7 during the tracking mission.

8 Defendant’s argument is premised on the assumption that the warrant was not facially
9 valid standing alone. As already noted, to be valid a warrant need only be based on probable
10 cause and describe with particularity the places to be searched and items to be seized. The
11 tracking warrant on its face satisfies these requirements. Having identified with particularity
12 the object of the search – the aircard – the warrant was not overbroad and did not need to be
13 cured by reference to the affidavit.

14 Moreover, the Court considered Agent Ng’s affidavit in the context of Defendant’s
15 argument that the government was required to provide additional details concerning the
16 operation of the mobile tracking device. The Court concluded, based on the affidavit, that
17 Judge Seeborg was adequately apprised of the nature of the technology. *See* Doc. 1009 at
18 24–25. Defendant does not dispute that Judge Seeborg was presented with Agent Ng’s
19 affidavit.

20 **B. Computer Search.**

21 Defendant asserts that the Court made the following errors in rejecting his challenges
22 to the government’s execution of the computer search protocol: (1) overlooking his
23 “temporal scope” argument; (2) overlooking the “core” of his minimization argument;
24 (3) finding that the government acted in good faith when relying on advice from the U.S.
25 Attorney’s office; (4) finding that the 30-day search window violations were not
26 “unattenuated but-for causes of obtaining digital evidence”; and (5) finding that there was
27 no Fourth Amendment violation “in light of IRS-CI Agent Daun waiting six months to start
28

1 her forensic examination while all other agents searched clones of the defendant's computer."
2 Doc. 1033 at 28–37.

3 (1) Defendant contends that agents reviewed information outside of the date range
4 on the warrant. Doc. 1033 at 28–30. The warrant authorized the seizure of evidence relating
5 to “possible violations of the following [enumerated] statutes . . . [f]or the period January 1,
6 2005, through the present.” *See* CR 845-2 at 4. Defendant argues that the government
7 exposed and reviewed all of the files on his “T” drive; 37,941 (out of a total of 53,521 files
8 reviewed) were dated prior to January 1, 2005. Doc. 1033 at 29. Defendant asserts that the
9 government's failure to abide by the temporal limits converted the warrant into a general
10 warrant. *Id.*

11 The government argues that the “temporal limitation applies to the violations being
12 investigated, not the type of evidence that may be relevant.” Doc. 1071 at 7. The Court
13 agrees. It reads the warrant as authorizing the seizure of data related to the enumerated
14 offenses, with the January 1, 2005, deadline referring to the date of the offense, not the date
15 of the files. As the government notes, “electronic copies of identity theft evidence, such as
16 birth certificates or lists of social security numbers, would have plainly been within the scope
17 of the warrant, even if those electronic copies were created prior to January 1, 2005.” *Id.*;
18 *see* Doc. 845-2 at 6, ¶ 3.

19 (2) Defendant argues that the Court erred by finding that the government did not
20 violate the minimization criteria set forth in the warrant. Doc. 1033 at 31. The computer
21 search protocol, incorporated into the warrant, required the government to “make all
22 reasonable efforts to use methods and procedures that will locate and expose only those
23 categories of files . . . that are identified with particularity in the warrant while, to the extent
24 reasonably practicable, minimizing exposure or examination of irrelevant, privileged, or
25 confidential files.” Doc. 464-3. According to Defendant, the government failed to do
26 “anything at all to comply with the minimization terms,” despite the fact that keyword
27 searches and other options were available to limit the scope of the search. Doc. 1033 at 31.
28

1 The Court found that Agent Daun's "human eye" view of the files did not violate the
2 protocol. Doc. 1009 at 41, n.10. The protocol requires only "reasonable" and "reasonably
3 practicable" means of limiting the scope of the computer search. Courts have consistently
4 recognized that "so long as the computer search is limited to a search for evidence explicitly
5 authorized in the warrant, it is reasonable for the executing officers to open various types of
6 files located in the computer's hard drive in order to determine whether they contain such
7 evidence." *United States v. Jack*, No. CR.S-07-266-FCD, 2009 WL 453051, at *4 (E.D.Cal.
8 February 23, 2009) (collecting cases); see *United States v. Giberson*, 527 F.3d 882 (9th Cir.
9 2008). Given the nature of the alleged criminal activities and the scope of materials
10 described in the warrant, the Court again finds that the search did not violate the
11 minimization requirements of the computer search protocol.

12 (3) Defendant argues that the Court erred in finding that the government acted in
13 good faith when it relied on the U.S. Attorney's office and its interpretation of the computer
14 search protocol. Doc. 1033 at 32. Specifically, Defendant asserts that the Court "ignored
15 binding Ninth Circuit precedent" in *Marks v. Clarke*, 102 F.3d 1012 (9th Cir. 1996).

16 *Marks* held that police officers were not entitled to qualified immunity when they
17 executed a facially invalid arrest warrant, notwithstanding the fact that the warrant was
18 reviewed by two Assistant U.S. Attorneys and signed by a magistrate. *Id.* at 1028. The
19 present case does not involve a facially invalid warrant, but the interpretation of the terms
20 of a computer search protocol by which a valid warrant was to be executed. The terms of the
21 protocol were subject to differing interpretations. The Court's original analysis was not
22 erroneous.

23 (4) Citing *Hudson v. Michigan*, 547 U.S. 586 (2006), Defendant argues that the
24 Court erred in finding that the "30-day search window violations were not unattenuated but-
25 for causes of obtaining digital evidence." Doc. 1033 at 32. Defendant contends that
26 government would not have obtained the data at issue if it had adhered to the 30-day search
27 limit set forth in the protocol. The Court disagrees.

1 In *Hudson*, the police officers had a valid search warrant for drugs and firearms, but
 2 entered Hudson's home in violation of the Fourth Amendment's knock-and-announce rule.
 3 The Supreme Court held that the violation did not warrant suppression of the evidence
 4 obtained from the search because the violation was not the unattenuated but-for cause of
 5 obtaining the evidence. The Court explained that "[w]hether that preliminary misstep had
 6 occurred *or not*, the police would have executed the warrant they had obtained, and would
 7 have discovered the gun and drugs inside the house." *Hudson*, 547 U.S. at 592. Here,
 8 contrary to Defendant's argument, the 30-day provision was not a hard deadline that would
 9 have prevented further examination of the data seized from Defendant. Even if the
 10 government had complied scrupulously with the deadline, the protocol itself provided that
 11 the government could obtain an extension of time to finish its search. Thus, violation of the
 12 deadline was not the but-for cause of the government obtaining the data.⁴

13 (5) Defendant argues that the Court committed manifest error when it found that
 14 no Fourth Amendment violation occurred despite the six-month delay in Agent Daun's
 15 forensic examination of the computer. Doc. 1033 at 36. For the reasons set forth in its prior
 16 order, the Court reiterates that these aspects of the computer search constituted technical
 17 violations of the search protocol and, under the circumstances of this case, do not warrant
 18 suppression under the Fourth Amendment. *See, e.g., United States v. Conrad*, No. 3:12-cr-
 19 134-J-34TEM, 2013 WL 4028273, at *8–10 (M.D.Fla. August 7, 2013).

20 C. Expectation of Privacy.

21 In addition to finding that Defendant's Fourth Amendment rights were not violated
 22 by the tracking warrant and the computer search, the Court evaluated whether Defendant met
 23 his burden of showing a reasonable expectation of privacy in the objects of the search.
 24 Defendant challenges the Court's conclusion that he did not have an objective expectation
 25 of privacy – i.e., "one that society is prepared to recognize as reasonable" – in his apartment,
 26

27 ⁴ The protocol provides that "[t]he deadlines . . . may be extended by court order
 28 for good cause shown." Doc. 464-3.

1 aircard, and computer. Doc. 1033 at 38–45. The Court reached this conclusion based on
2 Defendant’s comprehensive and multi-layered use of false identities, including those of real,
3 living individuals, which Defendant used to procure the items that were used in his scheme.
4 Other factors were also considered, such as Defendant’s readiness to abandon the apartment
5 on short notice and the nature of the electronic intrusion, which responded to Defendant’s
6 electronic implements of fraud.

7 Defendant challenges the Court’s finding that he lacked a legitimate expectation of
8 privacy in his apartment. First, Defendant disputes many of the factual determinations on
9 which the Court’s analysis was based. As discussed above, the alleged errors do not affect
10 the Court’s legal conclusions.

11 Defendant next argues that the Court erred by finding that he lacked a legitimate
12 expectation of privacy in his apartment because he was not “legitimately on the premises.”
13 Specifically, Defendant contends that the Court erred in its application of *Rakas v. Illinois*,
14 439 U.S. 128 (1978), and *United States v. Cunag*, 386 F.3d 888 (9th Cir. 2004). The Court
15 does not agree for reasons explained in detail in its prior order. *See* Doc. 1099 at 7-14. The
16 fact that Defendant disagrees with the Court’s analysis does not provide a basis for
17 reconsideration. A motion for reconsideration should not be used to ask the Court to rethink
18 its analysis. *Arizona Dream Act Coalition*, --- F. Supp.2d ---, 2013 WL 2128315, at *25.

19 Finally, Defendant argues that the Court erred in its analysis of his argument that he
20 had a “possessory and property interest in his aircard and computer.” Doc. 1033 at 44. Even
21 if the Court were to conclude that Defendant had legitimate property or possessory interests
22 in the items, and that such an interest gave rise to Fourth Amendment protections beyond
23 those arising from a reasonable expectation of privacy, these items were searched and seized
24 pursuant to valid warrants. No Fourth Amendment violation occurred.

25 **D. Other Alleged Manifest Legal Errors.**

26 Defendant argues that the Court erred by ignoring two of the issues raised in his
27 motions. First, Defendant asserts that it was manifest error for the Court to “completely
28

1 ignore the defendant's arguments relating to the N.D.Cal. 08-90331 MISC-RS Pen/Trap order
2 used to force the aircard to generate real-time cell site information." Doc. 1033 at 45.

3 In his motion to suppress, Defendant asserted that the 08-90331 order was invalid
4 because it was not supported by a finding of probable cause and because the agents exceeded
5 its scope. Doc. 824-1 at 314–15. The order authorized the installation of a pen register or
6 trap and trace device under 18 U.S.C. § 3122(b), which requires a showing that the
7 "information likely to be obtained is relevant to an ongoing criminal investigation," as well
8 the collection of cell phone records under 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d) of the
9 Stored Communications Act ("SCA"), based on "specific and articulable facts showing that
10 there are reasonable grounds to believe that the records . . . are relevant and material to an
11 ongoing criminal investigation." (Doc. 470-2.)

12 Because such "hybrid" orders potentially allow the government to obtain real-time cell
13 site location data without a showing of probable cause, their validity is an unsettled question.
14 *See, e.g., United States v. Espudo*, --- F.Supp.2d ----, 2013 WL 3803912 (S.D.Cal. 2013).
15 In the present case, however, the government ultimately located the aircard through its use
16 of mobile tracking devices as authorized by the tracking warrant upon a showing of probable
17 cause. In addition, the government's reliance on the order was objectively reasonable and
18 subject to the good faith exception. *Id.* at *14.

19 Finally, Defendant asserts that it was manifest error for the Court to "completely
20 ignore" his arguments concerning the destruction of evidence. Doc. 1033 at 46. Defendant
21 raised this issue in a supplemental motion to suppress, Doc. 830-2, and the Court addressed
22 it briefly in its order denying the motion, finding that the government's alleged destruction
23 of data was, at most, a technical violation for which suppression was an inappropriate
24 remedy. Doc. 1009 at 46. Defendant does not challenge this determination.

25 **IT IS ORDERED:**

- 26 1. Defendant's motion for reconsideration (Doc. 1033) is **denied**.
27 2. Defendant's request for an evidentiary hearing (Doc. 1038) is **denied**.
28

